

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### Protection du patrimoine intellectuel... un débat dépassé ?

Dieng, Dominique

*Published in:*  
Proceedings IES 2016

*Publication date:*  
2016

*Document Version*  
le PDF de l'éditeur

[Link to publication](#)

*Citation for pulished version (HARVARD):*

Dieng, D 2016, Protection du patrimoine intellectuel... un débat dépassé ? Dans *Proceedings IES 2016.*, 22, 13ème Forum européen IES 2016, Rouen, France, 5/10/16.

#### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



# Protection du patrimoine intellectuel ... un débat dépassé ?

Dominique DIENG<sup>1</sup>, AKASIAS, dominique.dieng@akasias.eu  
IES 2016 - 22, 6 octobre 2016

## Résumé

Open Source, Open Innovation, Open Science, Open Access, ... autant de paradigmes prônant le partage ... et qui constituent aujourd'hui l'environnement du chercheur. Dans un tel foisonnement « culturel », comment le chercheur, comment les institutions de recherche, peuvent-elles trouver leur chemin entre ouverture, partage des données, d'information, des résultats de recherche et protection de ce patrimoine ? Si le chercheur, le créateur est tenté de céder aux chants des sirènes de la stratégie Open, laquelle n'est pas toujours cette merveilleuse histoire qu'on voudrait nous faire accroire, il est important toutefois qu'il protège son patrimoine immatériel : ce qui n'est pas incompatible avec l'ouverture. Au-delà de la propriété intellectuelle et d'autres mesures juridiques, mesures immatérielles pour protéger des actifs immatériels, il existe également des mesures plus concrètes à mettre en place et qui vont de la protection du système informatique, à la gestion des déplacements en passant par l'accueil des stagiaires et des visiteurs...

**Mots-clés** : intelligence stratégique, intelligence économique, open innovation, open science, open access, open data, open source, protection de l'information, protection du patrimoine immatériel, patrimoine intellectuel, actifs immatériels.

## 1. Introduction

En mai 2016, la Commission européenne publiait l'ouvrage « Open innovation, Open Science, Open to the world »<sup>2</sup>, reflet de la vision stratégique du Commissaire Moedas, en charge de la Recherche, de la Science et de l'innovation. En préambule du chapitre « Open Science », on trouve cette vision du futur :

*« The year is 2030. Open Science has become a reality and is offering a whole range of new, unlimited opportunities for research and discovery worldwide. Scientists, citizens, publishers, research institutions, public and private research funders, students and education professionals as well as*

*companies from around the globe are sharing an open, virtual environment, called The Lab.*

*Open source communities and scientists, publishing companies and the high-tech industry have pushed the EU and UNESCO to develop common open research standards, establishing a virtual learning gateway, offering free public access to all scientific data as well as to all publicly funded research.*

*The OECD as well as many countries from Africa, Asia, and Latin America have adopted these new standards, allowing users to share a common platform to exchange knowledge at a global scale.*

<sup>1</sup> AKASIAS, Conseil en Intelligence stratégique, AKASIAS, [dominique.dieng@akasias.eu](mailto:dominique.dieng@akasias.eu), [www.akasias.eu](http://www.akasias.eu)

<sup>2</sup> E.C. - D.G. Research & Innovation, Open Innovation, Open Science, Open to the World, 2016.

*High-tech start-ups and small public-private partnerships have spread across the globe to become the service providers of the new digital science learning network, empowering researchers, citizens, educators, innovators and students worldwide to share knowledge by using the best available technology.*

*Free and open, high quality and crowd-sourced science, focusing on the grand societal challenges of our time, shapes the daily life of a new generation of researchers. »<sup>3</sup>*

Open Source, Open Innovation, Open Science, Open Access... autant de paradigmes prônant l'ouverture, le partage, la co-création, le libre accès et/ou la gratuité et qui, aujourd'hui, constituent l'environnement du chercheur. Face à un tel foisonnement, comment le chercheur, comment les institutions de recherche, peuvent-elles trouver leur chemin entre ouverture, partage des données, d'informations, des résultats de recherche et protection de ces biens immatériels qui constituent leur patrimoine ? Au-delà de la propriété intellectuelle, quelles mesures peuvent être mises en place pour protéger ce capital immatériel ? Cette description de l'avenir de l'*open science* portée par la Commission européenne : visionnaire ou utopique ?

Quelques-unes des questions auxquelles nous tenterons d'apporter une réponse après avoir rappelé les différents concepts et les raisons qui ont motivé les pouvoirs publics à soutenir, voire imposer ces stratégies d'ouverture. Nous examinerons les avantages et risques de ce mouvement pour la recherche et l'innovation à l'heure où institutions et laboratoires de recherche courent après les financements puis reviendrons à une réalité bien concrète : celle des risques auxquels sont confrontés les centres de recherche au quotidien. Nous illustrerons ces risques, qui vont bien au-delà de l'atteinte aux droits de propriété intellectuelle et dont les chercheurs et les institutions de recherche sous-estiment largement les impacts. Enfin, nous recommanderons des mesures susceptibles d'être mises en place pour en limiter les effets et concluons sur le véritable défi qui consiste à trouver l'équilibre entre la culture de la libre circulation de l'information et des connaissances et la protection du patrimoine du chercheur/des institutions de recherche.

---

<sup>3</sup> ibidem, p. 36

<sup>4</sup> Bush V., Science The Endless Frontier : A Report to the President by Vannevar Bush, Director of the Office of Scientific Research and Development, July 1945 (United States Government Printing Office, Washington: 1945)

## 2. Un peu d'histoire et quelques définitions

---

La convergence des technologies numériques, de nouveaux usages de partage de l'information à travers les réseaux sociaux, d'une volonté de la communauté scientifique de partager les résultats de la science au profit de son avancée... et en ce qui concerne l'*open science*, de la volonté de faire front contre l'hégémonie des éditeurs scientifiques et les prix prohibitifs des abonnements aux revues scientifiques qui limitent l'accès aux publications, constituent les premiers fondements du mouvement « Open ». Au-delà de cela, plus profondément, un mouvement irréversible, lié aux crises économique et financières, à la prise de conscience de la raréfaction des ressources et du changement climatique, est en marche : le changement sociétal et culturel qui, telle une vague de fond, est en train de bouleverser la société, ses valeurs et est sous-tendu par un retour à une économie de partage ... contribue à ce mouvement. En découlent les corollaires suivants : une plus grande ouverture de la science au profit de l'humanité, une meilleure intégration de l'humain dans le processus d'innovation par l'implication des différents acteurs, dont les usagers, dans la conception, la création, le développement et la commercialisation. Enfin, la volonté de faire face à la défiance des citoyens en instituant plus de transparence dans la gouvernance des entreprises et des pouvoirs publics alimente la spirale d'ouverture et ce mouvement qui s'accélère, vers toujours plus d'ouverture ne rencontre pas de réelle contestation.

### 2.1. L'Open Science

La plupart des auteurs convergent pour situer la naissance du mouvement Open Science dans les années 90 avec l'essor d'internet. Pourtant, déjà en 1945, à l'issue de la Seconde Guerre mondiale, Vannevar Bush<sup>4</sup>, conseiller scientifique du Président Roosevelt, invitait ce dernier à mettre à disposition des entreprises et de l'enseignement les résultats des travaux de recherche effectués pendant la guerre, particulièrement dans le domaine médical. Il était convaincu de ce que la capacité des USA à

sur National Science Foundation,  
<https://www.nsf.gov/od/lpa/nsf50/vbush1945.htm>  
(dernière consultation : 25/08/16)

surmonter l'ennemi dépendrait des progrès scientifiques : ils seraient plus rapides avec une politique de diffusion des connaissances plutôt que dans le cadre d'une politique de restriction.

*« Much of the information and experience acquired during the war is confined to the agencies that gathered it. Except to the extent that military security dictates otherwise, such knowledge should be spread upon the record for the benefit of the general public.*

*Thanks to the wise provision of the Secretary of War and the Secretary of the Navy, most of the results of war-time medical research have been published. Several hundred articles have appeared in the professional journals; many are in process of publication. The material still subject to security classification should be released as soon as possible.*

*It is my view that most of the remainder of the classified scientific material should be released as soon as there is ground for belief that the enemy will not be able to turn it against us in this war. Most of the information needed by industry and in education can be released without disclosing its embodiments in actual military material and devices. Basically there is no reason to believe that scientists of other countries will not in time rediscover everything we now know which is held in secrecy. A broad dissemination of scientific information upon which further advances can readily be made furnishes a sounder foundation for our national security than a policy of restriction which would impede our own progress although imposed in the hope that possible enemies would not catch up with us.*

*Our ability to overcome future enemies depends upon scientific advances which will proceed more rapidly with diffusion of knowledge than under a policy of continued restriction of knowledge now in our possession.»*

La Commission européenne définit l'*Open Science* comme une nouvelle approche du processus scientifique basée sur le travail coopératif et de nouvelles façons de diffuser la connaissance à travers l'usage des technologies numériques et de nouveaux outils collaboratifs<sup>5</sup>. Cette définition peut être complétée par celle qu'en donne le portail FOSTER<sup>6</sup> consacré à l'*open science*, à savoir qu'il s'agit de faire de la science de manière à ce que les autres puissent collaborer et contribuer. Dans

l'*open science*, données de recherche, notes de

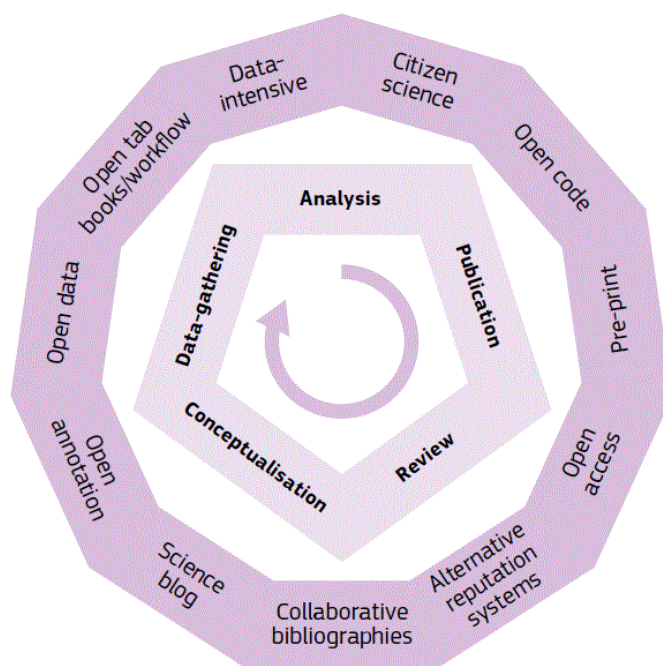


Figure 1 - Open Science: Opening up the research process

laboratoire, et autres processus de recherche sont disponibles gratuitement, dans des conditions qui permettent la réutilisation, la redistribution et la reproduction des résultats de la recherche ainsi que des données et méthodes qui la sous-tendent.

Ce premier paradigme en couvre bien d'autres toujours axés sur le partage de la connaissance et la collaboration à travers l'utilisation des technologies de l'information et de la communication. Le schéma ci-contre reprend les différents concepts tels qu'identifiés par la Commission Européenne<sup>7</sup>. Nous décrirons plus en détail ceux qui, aujourd'hui, circulent le plus : l'Open Access, l'Open Source et l'Open Data.

### 2.1.1. L'Open Access



Le mouvement Open Access qui vise la mise à disposition gratuite et/ou libre sur internet des publications scientifiques, a été officiellement lancé par la Déclaration de Berlin de 2003<sup>8</sup>.

<sup>5</sup> E.C., D.G. Research & Innovation, Open Innovation, Open Science, Open to the World, 2016, p. 33

<sup>6</sup> FOSTER (Facilitate Open Science Training for European Research), <https://www.fosteropenscience.eu/foster-taxonomy/open-science-definition> (dernière consultation : 25/08/16).

<sup>7</sup> E.C., D.G. Research & Innovation, Open Innovation, Open Science, Open to the World, 2016, p. 36 - Source : E.C., D.G. RTD & D.G. CONNECT, Public Consultation « Science 2.0: Science in transition » - Background document, 2014.

<sup>8</sup> Berlin Declaration on Open Access, 2007.

Celle-ci entérinait l'initiative de Budapest<sup>9</sup> sur l'Open Access signée l'année précédente laquelle, en 2012, réaffirmait le principe suivant : « *la littérature qui devrait être accessible en ligne gratuitement est celle que les savants donnent au monde sans en attendre de rétribution - les articles scientifiques revus par les pairs- [...] Par "accès libre" à cette littérature, nous entendons sa mise à disposition gratuite sur l'Internet public, permettant à tout un chacun de lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces articles, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale, sans barrière financière, légale ou technique autre que celles indissociables de l'accès et l'utilisation d'Internet. La seule contrainte sur la reproduction et la distribution, et le seul rôle du copyright dans ce domaine devrait être de garantir aux auteurs un contrôle sur l'intégrité de leurs travaux et le droit à être correctement reconnus et cités* ».

L'article 29 du Grant Agreement conditionne le financement des projets de recherche dans le cadre du programme Horizon 2020<sup>10</sup> à la diffusion en *open access* de toutes les publications scientifiques relues par des pairs dès lors qu'elles ont trait aux résultats. Il précise qu'elles doivent être gratuites et mises en ligne pour tout utilisateur.

### 2.1.2. L'Open Source



Le concept d'*open source* s'applique, quant à lui, aux logiciels. Le mouvement Open Source est né d'une scission, en 1998, avec la communauté du logiciel libre qui, pour sa part, prônait un modèle économique basé sur la vente des licences d'utilisation alors que les tenants de l'*open source* préféraient, quant à eux, promouvoir un modèle économique basé sur la vente des prestations. Cependant, derrière ces deux approches, se profile un objectif similaire à savoir

laisser l'accès ouvert aux codes sources des programmes informatiques développés.

Un rapport du Sénat français<sup>11</sup> en donne la définition suivante : « *la désignation open source, ou « code source ouvert », s'applique aux logiciels dont la licence respecte des critères précisément établis par l'Open Source Initiative, c'est-à-dire les possibilités de libre redistribution, d'accès au code source et de création de travaux dérivés. Mis à la disposition du grand public, ce code source est généralement le résultat d'une collaboration entre programmeurs* ».

### 2.1.3. L'Open Data

Le concept d'*Open Data*, lié à l'ouverture des données publiques et issu de la communauté scientifique, a été mentionné pour la première fois en 1995 dans un document du National Research Council relatif à l'ouverture des données géophysiques et environnementales<sup>12</sup>. Les auteurs estimaient que le caractère transfrontalier des phénomènes observés et les risques de privatisation des connaissances justifiaient cette ouverture des données.

En 2003, la Commission européenne édite la Directive sur la réutilisation de l'information du secteur public<sup>13</sup>, révisée en 2013. Elle vise à encourager les états, membres de l'Union européenne, à mettre à disposition des entreprises et des chercheurs les données détenues par les administrations publiques et les institutions financées par des fonds publics, y compris les musées, bibliothèques et archives.

En 2004, l'OCDE promulguait une déclaration selon laquelle les archives publiques des états membres devaient être rendues disponibles au public. En 2007, elle publiait des recommandations pour l'accès aux données de la recherche financée par des fonds publics<sup>14</sup>.

Le mouvement de l'Open Data a été pour sa part officiellement lancé en 2007 et s'inscrit dans la droite ligne du mouvement du logiciel libre. Son

<sup>9</sup> Budapest Open Access Initiative (BOAI), 2002, réaffirmée en 2012, [www.budapestopenaccessinitiative.org](http://www.budapestopenaccessinitiative.org) (dernière consultation : 25/08/16).

<sup>10</sup> H2020 Programme - Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020.

<sup>11</sup> Wikipédia : Open source [https://fr.wikipedia.org/wiki/Open\\_source](https://fr.wikipedia.org/wiki/Open_source) (dernière consultation : 28/08/16)

<sup>12</sup> CHIGNARD S., Open data - Comprendre l'ouverture des données publiques, FYP éditions, France, 2012 in *La protection des données personnelles dans l'open data* :

*une exigence et une opportunité* - Titre liminaire : une réflexion nécessaire, Rapport d'information du Sénat, <http://www.senat.fr/rap/r13-469/r13-4693.html> (dernière consultation : 28/08/16).

<sup>13</sup> Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public.

<sup>14</sup> OECD Principles and Guidelines for Access to Research Data from Public Funding as a soft-law recommendation, 2007.



moteur ? Un souhait de transparence et de valorisation des données des administrations publiques par les acteurs de la recherche et de l'innovation. Aujourd'hui, nombre d'administrations publiques de par le monde ont rejoint ce mouvement qui désormais s'étend également à des multinationales privées qui commencent à mettre à disposition du citoyen certaines de leurs données, au profit de la co-création, un moyen d'accélérer la création de nouveaux produits et services ou de l'amélioration de la satisfaction des clients. Procter & Gamble, Unilever ont relevé le gant et semble-t-il, à leur profit.

Dans son guide sur l'accès ouvert aux publications scientifiques<sup>15</sup>, la Commission européenne regroupe sous le vocable *open data* toute information, notamment des faits ou des chiffres, collectés pour être analysés et servir de base au raisonnement, à la discussion ou au calcul. La plateforme Foster<sup>16</sup>, quant à elle, insiste sur la gratuité de la mise à disposition en ligne et sur l'utilisation, la réutilisation, la distribution possible de ces données pourvu que la source des données soit mentionnée et partagée.

## 2.2. L'Open Innovation

L'*open innovation* a cela de commun avec l'*open science* qu'elles sont toutes deux portées par les technologies numériques et qu'elles sont parties d'une volonté de plus d'ouverture, de collaboration et d'une approche plus globale, plus intégrée.

Elle a été conceptualisée par Chesbrough<sup>17</sup> en 2003. Ce dernier défend le principe selon lequel de nos jours, les entreprises ne peuvent plus se permettre de compter uniquement sur leurs propres idées pour progresser - et qu'elles pourraient tirer meilleur parti de l'utilisation de leurs idées et technologies et de celles des autres qui font partie de leur cœur de métier. Selon lui, il n'y a pas un seul chemin pour amener une innovation sur le marché. Quant aux idées nées au sein de l'entreprise et non abouties elles pourraient être exploitées par d'autres.

Pour définir ce concept, un rapport de la Commission européenne sur l'*open innovation* et le transfert de connaissances<sup>18</sup> évoque « *des écosystèmes d'innovation multi-collaborative dans lesquels une innovation spécifique ne peut être vue comme une activité isolée qui ne tiendrait pas compte de son impact sur l'environnement économique et social* ». La co-création, développement conjoint de connaissances dans le cadre de relations développées avec des partenaires spécifiques, est au service de l'*open innovation*. Ce processus peut réunir autour d'un même projet, au sein d'un *living lab* ou laboratoire ouvert, un consortium de concurrents, de fournisseurs, de clients aussi bien que d'universités ou d'organisations publiques de recherche et des utilisateurs finaux. Cette coopération est caractérisée par de profondes interactions entre les partenaires et s'inscrit généralement dans la durée. Dans la même logique, on retrouve les *fab lab* ou laboratoires de fabrication, lieux ouverts, où matériel et outillage sont partagés : ils contribuent à accélérer la mise sur le marché en facilitant le prototypage, la mise au point des produits.

Aujourd'hui, c'est donc dans ce contexte d'ouverture, de collaboration, de co-création que Science et Innovation doivent trouver leur chemin. La plupart des auteurs font le panégyrique de ce mouvement d'ouverture et de partage des données et des résultats de la science, des administrations publiques. Mais tout est-il si parfait ?

## 3. Bénéfices et risques de l'ouverture

### 3.1. Bénéfices de la stratégie Open tels que vus par ses tenants

Les tenants de l'*open science* et de l'*open innovation* défendent les arguments suivants :

La connaissance mise à disposition de tous va permettre d'accélérer le progrès scientifique au

<sup>15</sup> E.C., H2020 Programme - Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020, Version 3.0, 26 July 2016.

<sup>16</sup> FOSTER (Facilitate Open Science Training for European Research), <https://www.fosteropenscience.eu> (dernière consultation : 25/08/16).

<sup>17</sup> CHESBROUGH H. W., Open Innovation : the new imperative for creating and profiting from technology, Harvard Business School Press, 2006.

<sup>18</sup> Commission européenne. (2014). Boosting Open Innovation and Knowledge Transfer in the European Union : independant expert group report on Open Innovation and Knowledge Transfer. Commission européenne. Bruxelles: European Union. doi:10.2777/65606.

bénéfice de l'humanité car elle autorise un chercheur à s'appuyer sur les résultats d'un autre pour les faire avancer et en améliorer la qualité. Elle évite de réinventer la roue, de répéter des erreurs similaires et limite donc la redondance des travaux. En permettant au chercheur, à l'innovateur, de solliciter ses pairs et/ou la société, elle accélère la résolution de problèmes et permet d'identifier les causes d'erreur susceptibles de bloquer l'avancement d'un projet. Polymath en est l'illustration de référence : en 2009, Tim Gowers, un mathématicien de l'Université de Cambridge, soumet à la communauté scientifique un problème mathématique qu'il ne pouvait résoudre. Trente-sept jours après la publication, non seulement le problème initial était résolu mais un problème plus complexe l'était également<sup>19</sup>. La stratégie Open se traduit par des économies d'échelle et, pour la recherche financée par des fonds publics, par un meilleur usage des deniers publics.

Les collaborations qui s'inscrivent dans l'approche Open sont tout bénéfice pour la recherche : elles renforcent la coopération internationale, elles favorisent l'interdisciplinarité, les collaborations intersectorielles et interinstitutionnelles. Elles gagnent de la co-création car elles permettent de créer des synergies autour d'un projet : ce qu'un chercheur mettrait dix ans à faire seul dans son laboratoire peut être réalisé en un an par dix chercheurs. Elles lui permettent également d'accéder à des sets importants de données auxquels, seul, il n'aurait jamais eu accès. Le Polar Data Catalogue<sup>20</sup>, cette base de données de métadonnées et de données qui décrit, indexe et donne accès à des sets de données est le fruit d'une collaboration entre chercheurs internationaux spécialistes de l'Arctique et de l'Antarctique. Le séquençage du génome humain est un autre exemple de recherche collaborative, qui a donné lieu à un ensemble d'accords, les Bermuda Principles<sup>21</sup>, qui visaient le partage immédiat par e-mail des séquences d'ADN identifiées.

Pour le chercheur, la publication de ses résultats en *open access*, est une opportunité pour sa visibilité internationale et pour renforcer son pouvoir d'influence : la collaboration scientifique internationale autour du changement climatique a montré quelles pressions les chercheurs réunis pouvaient exercer sur les décisions politiques -

même si le combat s'avère parfois rude et nécessite temps et patience.

L'*open science* présente une opportunité pour les chercheurs des pays en voie de développement qui peuvent ainsi bénéficier, à moindre coût, des résultats des laboratoires occidentaux. A leur tour, ils ont la possibilité de publier et de donner de la visibilité à leurs travaux, les plateformes *open access* leur permettant d'accéder gratuitement ou à des coûts abordables à la publication.

Dans des situations d'urgence et de crise humanitaire, l'*open science* peut s'avérer d'un grand secours. L'exemple de la pandémie du virus Ebola<sup>22</sup> illustre bien comment l'ouverture de la science et la collaboration scientifique peuvent se lier pour lutter contre une pandémie : cinq mois après le pic de l'épidémie, en avril 2014, une équipe internationale de chercheurs a séquencé 3 génomes du virus et rendu immédiatement publics ces résultats ; deux mois après, le Broad Institute (Cambridge, Massachusetts, USA) en séquence 99. Trois ans après le début de la pandémie l'Organisation Mondiale de la Santé annonçait la fin de la transmission du virus (même s'il reste quelques cas sporadiques). L'Humanitarian OpenStreetMap Team (HOT) dont l'objectif est de répondre aux problèmes humanitaires en cartographiant les voies d'accès s'appuie sur l'*open source* et l'*open data* : en 2010, la mobilisation rapide de ses membres et leur intervention en Haïti après un tremblement de terre de magnitude 7.0 a contribué à sauver de nombreuses vies humaines.

L'accélération du transfert des résultats de la recherche active le processus d'innovation, l'entrée sur le marché au bénéfice de la croissance économique.

La stratégie Open s'inscrit dans un processus démocratique qui, à travers plus de transparence et un renforcement de la collaboration de tous les acteurs de la société civile, permet de donner voix au chapitre au citoyen : celui-ci sera plus impliqué dans la vie politique, économique et sociale. Tenant compte des besoins qu'il aura formulés, tant l'efficacité et la performance de la recherche et l'innovation s'en trouveront améliorées et permettront de répondre aux défis sociétaux : rencontrant mieux les attentes du citoyen, elles ne pourront trouver meilleur ambassadeur que ce dernier et, la boucle étant bouclée, meilleur

<sup>19</sup> <http://polymathprojects.org> in E.C., D.G. Research & Innovation, Open Innovation, Open Science, Open to the World, 2016.

<sup>20</sup> <https://www.polardata.ca/> (dernière consultation : 31/08/16).

<sup>21</sup> Bermuda principles, 1996, <http://dukespace.lib.duke.edu/dspace/handle/10161/7407> (dernière consultation : 01/09/16)

<sup>22</sup> YOZWIAK N.L. et al (2015), Make outbreak research open access, Nature, vol. 518, 26 février 2015, p. 479.

sponsor, en qualité de consommateur et/ou d'investisseur par, exemple, à travers le *crowdfunding* ou financement participatif.

Autre retombées économiques ? La réutilisation des données publiques, qui permet à des entreprises de s'en « approprier » pour les transformer, les reconditionner en de nouveaux produits et services, est génératrice de nouveaux marchés, de nouveaux revenus et par là même, créatrice d'emplois. La mise à disposition des « inventions dormantes » dont un laboratoire de recherche, une entreprise ne savait que faire permet à d'autres de les exploiter et donc de créer également de la valeur.

Enfin, la stratégie Open favorise le processus d'idéation permettant au chercheur, au créateur de s'inspirer d'idées, de méthodes, concepts issus d'autres disciplines pour les intégrer dans sa propre discipline et ainsi innover...

L'engouement pour les stratégies Open, les résultats positifs que ces pratiques ont permis d'obtenir ne doivent pas occulter le revers de la médaille. Or, hormis les spécialistes de la propriété intellectuelle, rares sont les auteurs à s'interroger sur les conséquences de cette stratégie d'ouverture. Peut-être parce que le mouvement est encore trop jeune et que l'on manque de recul pour en évaluer les impacts, peut-être parce qu'il y a un effet d'entraînement et que toutes les organisations publiques et privées, Commission européenne y comprise, se trouvent coincées dans une spirale - Effet de mode ? Idéalisme ? - qui les entraîne à aller de l'avant et à développer ce nouveau paradigme, dans une croyance selon laquelle la stratégie Open va tout résoudre. On ne peut que les inviter à prendre le recul nécessaire pour anticiper, évaluer les impacts négatifs potentiels et penser contre-mesures.

### 3.2. Tout n'est pas tout rose dans le monde de l'Open

Le spécialiste de l'intelligence stratégique est interpellé à plusieurs niveaux : le devenir de son métier de veilleur dans un environnement où un des éléments qui constituait sa valeur ajoutée à savoir sa capacité à trouver l'information « rare » est remis en question. Encore que l'invitation de Chesbrough à aller chercher les idées ailleurs puisse

plaider pour le veilleur. Quoi qu'il en soit, s'il convient de souligner ce changement à venir, ce n'est cependant pas l'objet de cet article. Nous mettons ici l'accent sur le second pilier de l'intelligence stratégique, à savoir la protection de l'information : celle-ci, largement oubliée ou limitée à la propriété intellectuelle, nous semble devoir revenir au centre du débat.

Certes, l'humanité dans son ensemble a beaucoup à gagner de l'ouverture et du partage. Mais si on redescend à l'échelle d'une nation et, un cran en dessous, à l'échelle du laboratoire, de l'entreprise ou du chercheur est-on bien sûr que ce soit tout bénéfique pour eux ? La publication des données de séquençage à un stade précoce de l'épidémie de MERS (Middle East Respiratory Syndrome) qui a frappé l'Arabie Saoudite en 2012 a mis en évidence les incertitudes relatives aux droits de propriété intellectuelle, et les conflits qui en sont nés ont entravé l'accès aux échantillons<sup>23</sup>. Dans des situations de crise telles que celle-là, l'incertitude quant à la propriété des données - appartiennent-elles au gouvernement ? Aux personnes qui en assurent la collecte ? - peuvent être un frein au partage de l'information et à l'avancement de la recherche. Cette question de la rémunération des chercheurs et des innovateurs devra être débattue.

Dans une interview portant sur la conférence « Géopolitique de l'open : les gagnants et les perdants », G. Chartron répondait à la question « Pourquoi ces termes "gagnants" et "perdants" ? », en ces mots : « *car le mouvement Open redistribue les cartes entre les acteurs. Les producteurs de contenus qui se rétribuaient hier sur des modèles d'abonnement des utilisateurs doivent retrouver des modèles économiques autres. Tout cela est encore très fragile notamment pour les plus petits acteurs. Le transfert de valeur se fait du contenu au contenant : on ne veut plus payer de contenus mais des sommes folles sont dépensées pour les équipements, les plateformes, les outils de fouille de données...* »<sup>24</sup>. Le mouvement Open détruit de la valeur en amont, les nouveaux modèles économiques qui en découlent permettront-ils d'en créer en aval ? Les nouveaux acteurs entrants qui développent des produits et services autour de l'agrégation de contenus, autour des prestations de service auront-ils les reins assez solides pour compenser les pertes en amont ?

L'engouement pour l'*open access* a mis sur le marché des publications en libre accès d'éditeurs dits « éditeurs prédateurs » qui, profitant de ce

<sup>23</sup> YOZWIAK N.L. et al (2015), Make outbreak research open access, Nature, vol. 518, 26 février 2015, p. 478

<sup>24</sup> CHARTRON G., in 3 questions à Ghislaine Chartron : les acteurs et l'impact du mouvement open, [www.mysciencework.com](http://www.mysciencework.com), 19 novembre 2014.



mouvement et de la multiplication des plateformes de publication, arnaquent les chercheurs et diffusent, pour certains d'entre eux, des articles sans aucune valeur scientifique. Ceci pose la question de l'éthique de la publication.

Aujourd'hui, la logique dominante n'est plus celle du « first to invent » ou du « first to patent » mais celle du « speed to market ». Dans l'*open innovation*, le facteur différentiel c'est la rapidité : rapidité à acquérir de nouvelles technologies, rapidité à développer de nouvelles innovations, et au bout du compte, rapidité à mettre sur le marché, à commercialiser. Ce qui est sous-tendu par la rapidité à détecter des opportunités. Il en va de même dans l'*open science*, rapidité à identifier les sources de financement en Europe et ailleurs dans le monde, connaissance des réseaux, des éditeurs en ligne pour se donner de la visibilité. Nos organisations, entreprises, centres de recherche, ne risquent-ils pas de se faire happer, dépasser par des structures ayant investi des ressources conséquentes pour assurer une veille internationale, comme c'est le cas au Japon, en Corée, et en Chine ? Dans toutes les universités chinoises, il existe une cellule de veille chargée de scruter les publications et innovations des autres pays. Et nous, où en sommes-nous ?

Dans un environnement hyperconcurrentiel, nos organisations sont-elles suffisamment agiles pour réagir et saisir les opportunités de développement économique, de valorisation des inventions et innovations qu'elles ont produites ? Sont-elles suffisamment agiles pour détecter à temps les opportunités des pays étrangers et les transformer en valeur au profit de nos nations ? Or c'est la rapidité de mise en œuvre et d'exécution qui va permettre de contrer la concurrence lorsqu'on connaît la capacité de réaction des entreprises asiatiques. Comme l'écrivent les auteurs du rapport « L'innovation : un enjeu majeur pour la France »<sup>25</sup>, « pendant quelques années, nous avons vécu dans le mirage d'une économie de la connaissance uniquement fondée sur la production de propriété intellectuelle et les services, et déléguant les activités de production à des pays moins développés... l'innovation, c'est aussi la production et cela suppose donc une industrialisation ... c'est bien l'exploitation en France qui permet de valoriser le mieux pour le pays les investissements publics et privés en R&D ». Dans le Global Innovation Index

2016<sup>26</sup>, la France occupe la 11<sup>ème</sup> place en termes de R&D et la 39<sup>ème</sup> en termes d'impact de la connaissance. La Belgique respectivement les 16<sup>ème</sup> et 46<sup>ème</sup> place tandis que l'Allemagne score à la 9<sup>ème</sup> place pour sa R&D et la 26<sup>ème</sup> pour l'impact économique. Les conditions sont-elles là pour retenir en Europe les *spin-offs* et *start-ups* nées au départ des inventions et innovations nationales et éviter que leur croissance ne servent les pays vers lesquels elles sont tentées de migrer ?

Face à des équipes de recherche qui atteignent des niveaux de compétence élevés, qui profitent de l'*open access* pour publier abondamment et bénéficient ainsi d'une visibilité accrue, qui sont nombreuses et dont les niveaux de rémunération sont bien inférieurs à ceux de la vieille Europe, ne risque-t-on pas un retour de manivelle ? Ces équipes de recherche risquent de faire de l'ombre à la recherche occidentale avec lesquelles elles entrent en compétition en attirant les fonds privés ... mais aussi certains fonds européens dans le cadre d'accords de coopération au nom d'un rêve selon lequel l'Europe va attirer des chercheurs étrangers qui, soit y resteront et feront bénéficier les pays européens de leur expertise, soit repartiront chez eux après avoir noué des liens qui s'inscriront dans la durée en faveur de coopérations futures.

Mais est-ce si simple ? Le jeu est-il parfaitement équilibré ? Sommes-nous à égalité sur tous les plans ? Un simple exemple : la Chine tout comme la Russie se sont engagées dans le mouvement *open data*. Seulement leurs bases de données sont respectivement en chinois pour la première et en caractère cyrillique pour la seconde : donc, certes l'accès est ouvert mais... il faut maîtriser ces alphabets pour pouvoir utiliser les données<sup>27</sup>. Sans compter les disparités en termes de qualité et d'exhaustivité des données qui ne plaident pas en faveur de l'égalité.

En permettant l'accès de tout à tous, ne met-on pas en péril nos économies ? Avons-nous les moyens de réagir suffisamment rapidement et de tirer profit des découvertes scientifiques développées sur nos territoires au bénéfice de nos entreprises et citoyens ?

Nous l'avons vu, un des enjeux de la stratégie Open dans un environnement compétitif, est d'assurer à la fois la protection du capital immatériel national

<sup>25</sup> BEYLAT J.-L. & TAMBOURIN P. & alii, L'innovation : un enjeu majeur pour la France : dynamiser la croissance des entreprises innovantes, Ministère du Redressement productif et Ministère de l'Enseignement supérieur et de la Recherche, avril 2013.

<sup>26</sup> Global Innovation Index 2016, <https://www.globalinnovationindex.org>.

<sup>27</sup> DA SILVA PIRES A., Découvrir la planète Open Data : l'ouverture pour quelle valeur ? Journal du Net, 29 janvier 2014.

et la valorisation de la recherche et de l'innovation générée sur le territoire national, au profit de l'industrie et de l'emploi tout en contribuant à l'ouverture internationale des résultats de la recherche et des données publiques. L'enjeu réside également dans la capacité de profiter des données mises en ligne par les autres pour créer de la valeur dans nos pays. Cela implique de disposer d'un dispositif de veille adéquat, de la capacité à rebondir rapidement et que les conditions, l'environnement économique permettant ce rebondissement soient en place. Cela suppose également que les chercheurs, les administrations publiques, avant de mettre en ligne leurs résultats, leurs données pèsent le pour et le contre et évaluent pour chaque donnée, si elle peut ou non être partagée. Cela implique aussi de protéger son capital immatériel, laquelle protection passe par des mesures juridiques mais pas uniquement.

## 4. Comment protéger ses actifs immatériels ?

---

*Open science* et *open innovation*, ouverture et libre accès à la connaissance, sont-ils antinomiques avec protection de la connaissance ? Nous ne pensons pas : que l'on soit ou non dans un processus de recherche ou d'innovation collaborative, il y a toujours une décision sur le **choix** de partager ou non l'information, sur le **degré de partage** que l'on souhaite, sur le **moment** de mise à disposition ou de partage et sur les **personnes** avec qui on souhaite opérer ce partage, le monde entier ou une groupe restreint de partenaires... C'est ce libre-arbitre qu'il convient de protéger et de faire respecter. Le chercheur, le laboratoire qui découvre que ses idées, les résultats de ses travaux de recherche ont été interceptés, utilisés, voire détruits par des personnes non autorisées avant même que lui-même ait décidé de ce qu'il en ferait ou n'ait pu les exploiter ne pourra que regretter de ne pas avoir pris les simples mesures de précautions préconisées ci-après.

Dans les faits, lorsque vous demandez à un chercheur ou à un valorisateur quelles sont les mesures de protection de la production intellectuelle prises au niveau du laboratoire ou de l'université, il ne manquera pas, très sûr de lui, de vous citer les droits de propriété intellectuelle. Et,

dans le cas d'un jeune chercheur - s'il vient de débiter ses travaux - que son domaine de recherche est si spécifique qu'il ne voit pas l'intérêt de protéger ses résultats et qu'il a tout au contraire intérêt à les diffuser, à communiquer. Trop souvent, les chercheurs associent la protection de leurs résultats de recherche au dépôt d'un brevet, au droit d'auteur ; en fait, la plupart du temps, ils pensent mesures de protection immatérielle pour un patrimoine immatériel. Or il existe d'autres mesures pour assurer la protection de ce patrimoine.

Nous allons nous atteler au périlleux exercice de synthétiser en quelques pages un ensemble de mesures dont la description détaillée remplirait des armoires<sup>28</sup> : notre objectif est de procéder à une piqure de rappel dans le but d'inviter le lecteur à évaluer les mesures qu'il pourrait mettre en place pour lui-même ou son laboratoire. Certaines se situent au niveau du laboratoire et/ou de l'institution et ont trait à la sécurité informatique, la protection des locaux, la gestion des ressources humaines et les mesures organisationnelles, la gestion des stagiaires et des visiteurs. D'autres renvoient au comportement individuel. Selon la discipline de recherche, certaines seront d'application, d'autres moins : en fait, elles dépendent des enjeux représentés par le patrimoine immatériel et de son potentiel de valorisation.

Nous ne prétendons pas à l'exhaustivité et évoquerons des mesures dont la mise en œuvre est relativement aisée. Notre volonté est celle d'attirer l'attention sur le fait que ... « non, cela n'arrive pas qu'aux autres » et que la question n'est pas « est-ce qu'un incident se produira ? » mais « quand l'incident se produira-t-il ? ». Enfin, recherche ouverte ou pas, n'est-il pas regrettable de perdre le fruit de mois de travail, voire de collaboration à cause d'une négligence ?

### 4.1. La protection juridique : les droits de propriété intellectuelle et les contrats

Le premier réflexe du chercheur lorsqu'on lui parle de protection de ses travaux de recherche est d'évoquer la protection juridique et notamment les droits de propriété intellectuelle tels que les brevets, le droit d'auteur, les dessins et modèles. Ces droits, « *conférés à l'individu par une création*

---

<sup>28</sup> Norme ISO 27001 sur les systèmes de management de la sécurité de l'information

intellectuelle... donnent généralement au créateur un droit exclusif sur sa création pendant une certaine période »<sup>29</sup>. Toutefois, élaborés au 19<sup>ème</sup> siècle, dans un contexte où une innovation pouvait facilement être attribuée à un auteur donné, ces mécanismes de protection sont-ils encore adaptés au contexte de l'*open innovation* et de l'*open science* ? Sont-ils adaptés à une situation où le processus de création fait appel à plusieurs auteurs qui vont travailler simultanément dans le cadre d'un processus collaboratif et/ou successivement dans le cadre de l'innovation donnant lieu à des produits dérivés ? Les juristes devront-ils, comme le préconisent certains auteurs, mettre plus d'agilité dans l'utilisation qu'ils font des droits de la propriété intellectuelle ?

Le libre-arbitre que nous évoquions plus haut est toutefois limité pour le chercheur participant à un projet financé par la Commission européenne dans le cadre du programme Horizon 2020 : l'art. 27 du Grant Agreement<sup>30</sup> impose l'obligation de protéger ses résultats pour une période et une couverture territoriale appropriée, dès lors qu'on peut raisonnablement espérer les exploiter commercialement ou industriellement - tout en imposant quelques lignes plus loin (art. 29) à les publier (sic !).

Les **licences Creative Commons**, complément au droit d'auteur, sont des alternatives à évaluer par le chercheur lorsqu'il envisage de partager ses publications ou le code source de logiciels qu'il a développés : elles permettent de définir les limites dans lesquelles il autorise l'utilisation de ses créations.

Il existe toutefois un droit de propriété intellectuelle très peu utilisé par les institutions et les centres de recherche et ce, à tort à notre avis, c'est le **droit des marques**. Le CNRS (France) est l'un des rares organismes de recherche à avoir conscience de l'importance de protéger sa marque et à l'avoir même déposée à l'international.

Un autre moyen de protéger les résultats de ses inventions et innovation, c'est le **secret d'affaires** que la proposition de Directive sur la protection des secrets d'affaires<sup>31</sup> définit ainsi : «*On entend par « secret d'affaires », des informations qui répondent à toutes les conditions suivantes :*

a) elles sont secrètes en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, elles ne sont pas généralement connues des personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou ne leur sont pas aisément accessibles;

b) elles ont une valeur commerciale parce qu'elles sont secrètes;

c) elles ont fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrètes;

Cette directive est-elle contradictoire avec l'innovation ouverte ou la recherche collaborative ? A priori non, car elle vise au contraire à favoriser la création intellectuelle et l'innovation en assurant leur protection contre l'obtention, l'utilisation ou la divulgation illicite par d'autres parties.

Enfin, il y a les conventions telles que les accords de confidentialité, les accords de consortium, dont il convient d'évaluer le coût-bénéfice en termes de facilitation de la collaboration avec les partenaires ou les fournisseurs. Avec ces derniers aussi, il est conseillé de prévoir une clause de confidentialité, comme l'a fait un centre de recherche, pour éviter qu'ils ne divulguent auprès d'autres clients, les fournitures livrées au centre de recherche : ces informations peuvent être de précieux indices sur les recherches en cours et s'avérer très utiles à un laboratoire directement concurrent ou à une entreprise concurrente d'un client du laboratoire.

Enfin, mentionnons, une mesure qui, si elle n'est pas juridique peut toutefois servir pour réclamer la paternité d'une information, particulièrement dans l'innovation collaborative, c'est la rédaction de comptes-rendus de réunion.

<sup>29</sup> Organisation Mondiale du Commerce, [https://www.wto.org/french/tratop\\_f/trips\\_f/intel1\\_f.htm](https://www.wto.org/french/tratop_f/trips_f/intel1_f.htm) (dernière consultation : 27/08/16).

<sup>30</sup> H2020 Programme Multi-Beneficiary General Model Grant Agreement (H2020 General MGA — Multi), Version 3.0, 20 juillet 2016.

<sup>31</sup> Résolution législative du Parlement européen du 14 avril 2016 sur la proposition de directive du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (COM(2013)0813 – C7-0431/2013 – 2013/0402(COD)).

## 4.2. La protection informatique

D'une étude du consultant Ernst & Young sur la sécurité (2015)<sup>32</sup>, il ressort que 44% des entreprises interrogées estiment que le *phishing* ou hameçonnage constitue LA plus grande menace et 43% que les logiciels malveillants sont au nombre des autres menaces les plus fortes qui pèsent sur leur organisation.

Les universités, les centres de recherche échapperaient-ils à cette règle et seraient-ils à l'abri de telles menaces ? L'actualité nous démontre qu'ils sont également des cibles. Mai 2016 : l'Université de Calgary (Canada) est victime d'un *ransomware* et doit déboursier une rançon d'environ 20.000 dollars canadiens en monnaie Bitcoin pour récupérer la maîtrise de ses serveurs de courrier électronique, bloqués pendant une dizaine de jours. Janvier 2016, l'université Tsinghua de Pékin (Chine) est la proie d'un pirate informatique : revendiquant son action au nom de l'Etat Islamique (EI / Daesch), il a modifié des pages du portail de cours en ligne les remplaçant par des versets de textes sacrés du Coran. Février 2015 : l'Université de Lyon 3 (France) subit une attaque sur une de ses bases de données : 88 000 contacts reprenant les données personnelles des étudiants et de son personnel sont dans la nature. Outre les noms, prénoms, dates de naissance, informations sur les cursus suivis, adresses personnelles, numéros d'étudiants, numéros de téléphone, les personnes concernées ont pu retrouver des historiques d'échanges de courriers électroniques entre membres du personnel de l'université, les coordonnées d'entreprises partenaires<sup>33</sup>. Début 2014, un professeur de l'Université Catholique de Louvain - UCL (Belgique), spécialiste de la cryptographie, fut victime d'une attaque « ciblée » suspectée d'avoir été portée par les services de renseignement d'un pays étranger. L'ordinateur de ce chercheur avait été infecté après qu'il ait cliqué sur une invitation LinkedIn reçue par e-mail : celle-ci émanait en fait d'une personne fictive. Ce dernier exemple illustre parfaitement où se situe l'une des failles les plus courantes du système d'information (les hommes... et les femmes) et conforte les craintes des entreprises à l'égard des tentatives de *phishing*.

Nous ne décrivons pas les mesures de sécurité à mettre en œuvre au niveau d'un service informatique. Ce n'est pas l'objet de cet article. Par contre, nous rappellerons les mesures que tout un

chacun peut prendre pour contribuer, à titre individuel, à la protection du système informatique et par là même à celle de son patrimoine intellectuel et de celui de son institution.

En premier lieu, un petit rappel : dans la mesure où les données, qu'il s'agisse de données scientifiques ou publiques, sont mises en ligne afin qu'elles puissent être réutilisées par d'autres, les producteurs de données (chercheurs, administrations publiques, ou acteurs du privé ...) ont une obligation qui pourrait engager leur responsabilité : celle de publier des informations de qualité et de veiller à la **disponibilité**, l'**intégrité**, la **confidentialité** des données et à l'**interopérabilité** des bases de données.

Il est important de sensibiliser les chercheurs :

- aux risques liés à l'ingénierie sociale, cette phase d'approche qui consiste à sympathiser par le canal des réseaux sociaux pour baisser les défenses de la personne ciblée et lui soutirer à son insu des informations qui peuvent s'avérer stratégiques et permettre d'infiltrer les réseaux et ordinateurs d'une organisation ;
- à l'utilisation de la clé USB qui, à l'insu de son propriétaire, peut capter du code piraté et infecter tous les ordinateurs sur lesquels elle sera installée. Ou qui, sciemment piégée, et remise par un « collègue » pour copier un fichier, va installer un malware sur l'ordinateur ;
- à l'utilisation de mots de passe suffisamment longs et régulièrement modifiés ;
- et aussi aux back-up réguliers. Car outre les attaques informatiques, nul n'est à l'abri d'un crash de disque dur ou d'un vol d'ordinateur : une unité de recherche d'une université belge a ainsi vu des mois de recherche totalement anéantis après le cambriolage de ses bureaux et le vol de l'ordinateur sur lequel ses résultats étaient consignés MAIS ... n'avaient pas été sauvegardés sur un autre serveur.

Mesures informatiques mais aussi protection du matériel et des locaux, la protection du patrimoine immatériel passe aussi par là.

<sup>32</sup> Ernst & Young, Cybersécurité : créer les conditions de la confiance dans le monde digital, 2015.

<sup>33</sup> PONCET G., Piratée, l'Université Lyon-3 veut renforcer sa cybersécurité, Le Point.fr, le 24/02/2015 (dernière consultation : 27/08/16).

### 4.3. La protection des locaux et du matériel

Un autre exemple illustratif de la réalité du terrain : un centre de recherche, un serveur de back-up posé à même le sol dans un local théoriquement fermé à clé mais dont la clé est « cachée » au vu et au su de tous (y compris des équipes de nettoyage), le local sert également de salle d'archivage pour les documents légaux. Une des équipes de recherche dont le labo occupe la salle voisine, sans en avoir averti le responsable informatique, installe dans ce local un climatiseur (nécessaire à ses manipulations) susceptible de condensation voire de fuites d'eau : chercher l' (les) erreur(s) !

La protection des locaux couvre plusieurs dimensions : la protection de l'accès au site même où est installé le laboratoire, la protection des locaux eux-mêmes, la gestion des accès et des déplacements, sans oublier la protection contre les sinistres. L'exemple d'un incident qui aurait pu mal tourner : des produits chimiques sensibles à l'eau stockés au premier étage d'un bâtiment ; un écoulement d'eau à l'étage au-dessus.

La **protection du site** lui-même passera par la mise en place d'obstacles physiques tels qu'une grille, un mur d'enceinte, des portes blindées, un éclairage « intelligent », la définition de zones réservées ou protégées à accès limité, le recours au gardiennage ou à la vidéosurveillance.

Quant à la **protection des locaux**, elle passe par le renforcement des portes et serrures, la protection des ouvertures, la mise en place de systèmes d'alarmes. Enfin la **gestion des accès**, devrait idéalement passer par l'utilisation d'un badge, la tenue d'un registre des visites et l'accompagnement des visiteurs.

Ces mesures de protection des accès ne sont pas toujours aisées à mettre en œuvre au sein des établissements universitaires qui, quotidiennement, accueillent des centaines de personnes (membres du personnel, étudiants, enseignants visiteurs, ...) ou dans des centres de recherche qui, travaillant en étroite collaboration avec des universités, accueillent étudiants et stagiaires nationaux ou étrangers.

### 4.4. L'accueil des visiteurs et des stagiaires

Il est courant, au sein des établissements de recherche, d'accueillir des professeurs ou des chercheurs visiteurs, des entreprises ou des stagiaires. Ils peuvent représenter une faille dans la protection des actifs immatériels d'une institution ou d'un laboratoire de recherche.

En mai 2005, l'ESISC (European Strategic Intelligence and Security Center) révélait au journal *Le Monde*<sup>34</sup> ses soupçons sur une association d'étudiants et de chercheurs hébergée par la Katholieke Universiteit Leuven (KU Leuven - Belgique) : celle-ci abritait un réseau international de renseignement économique constitué de près de 800 étudiants, chercheurs, professeurs et stagiaires chinois ; le réseau avait, au départ de la Belgique, des ramifications en France, en Grande-Bretagne et en Allemagne. L'article du Monde révèle également une autre tentative d'espionnage qui s'est déroulée le même mois en Suède : des scientifiques chinois admis au Karolinska Institutet (Suède) ont été pris en flagrant délit de tentative d'obtention frauduleuse d'informations sur des découvertes non brevetées.

Au niveau de l'**accueil des visiteurs**, le port d'un badge « visiteur » obligatoire et aisément reconnaissable est une des premières mesures incontournables. Dans le cas de recherches très sensibles ou de discussions hautement confidentielles, on interdira l'introduction d'un *device* mobile (appareil photo, téléphone, voire même ordinateur). Etant donné la miniaturisation des *devices*, cela ne garantit rien mais minimise néanmoins les risques. On pensera également à mettre en place un **parcours de notoriété**, qui évite que des visiteurs aient accès à des recherches en cours (vue sur les écrans, sur des prototypes, des cultures). On vérifiera également les informations affichées sur les panneaux d'information à destination du personnel. Enfin le chercheur hôte se méfiera des questions anodines relatives à d'autres services et refusera systématiquement de répondre à des demandes d'information concernant d'autres services.

Au niveau de l'**accueil des stagiaires** : on prévoira des conventions de stage intégrant systématiquement une clause de confidentialité et une clause relative à la propriété intellectuelle. Avant le démarrage du stage, le directeur de stage

<sup>34</sup> STROOBANTS J.-P., Une université belge pourrait abriter un réseau d'espionnage industriel chinois, LE MONDE, 10.05.2005, Mis à jour le 18.12.2007.



s'assurera que le stagiaire a bien compris ses engagements et responsabilités ainsi que les sanctions qui découleraient du non-respect de ses obligations. Il s'assure également que l'accès à l'intranet et les permissions soient limitées, et que les comptes soient clôturés sitôt le stagiaire parti.

#### 4.5. Les collaborateurs

Il est important de sensibiliser les chercheurs à la **valeur** des informations dont ils sont à la source car, bien souvent, c'est le cadet de leurs soucis. Il s'agit de faire des collaborateurs des partenaires co-responsables de la protection du patrimoine du labo car en matière de protection de l'information, le maillon faible ce sont les hommes ... et les femmes. Dans l'enquête 2015 d'Ernst & Young<sup>35</sup>, 44% des entreprises sondées ont le sentiment d'être vulnérables à cause de salariés non sensibilisés ou négligents, et 27% qu'elles sont susceptibles d'être victimes d'attaques internes menées par des salariés mécontents.

La sensibilisation commence avec le **contrat de travail** qui contiendra au minimum une clause de confidentialité, une clause de propriété intellectuelle. Il comprendra également une clause de restitution des données confidentielles et du matériel ainsi qu'une clause de non concurrence, en cas de départ. Elle se poursuit avec le **règlement de travail** qui précise les points relatifs à l'utilisation du matériel et la politique de l'organisation en matière de BYOD (Bring your Own device), d'utilisation du Cloud computing et des réseaux sociaux. Il mentionne les règles à respecter en termes de comportement au sein de l'institution et précise l'attitude à avoir en cas de sollicitations de personnes se présentant comme journalistes (un moyen détourné d'obtenir de l'information). Enfin il mentionne les responsabilités de chacun dans le processus de protection de l'information et rappelle les sanctions légales notamment celles qui frappent la divulgation d'informations confidentielles acquises dans le cadre de la relation de travail.

La prise de conscience se poursuit au travers des **formations** ou des actions de **sensibilisation**, voire des exercices de simulation sur les points que nous avons mentionnés précédemment. A titre d'exemple, pour sensibiliser les chercheurs aux risques d'hameçonnage, le responsable informatique d'un centre de recherche a fait un exercice de simulation avec un e-mail demandant les codes d'accès des collaborateurs : près d'un tiers

des collaborateurs sollicités le lui ont communiqué. Ce fut l'occasion de faire le point par la suite et de les sensibiliser.

#### 4.6. La gestion des déplacements

La protection du patrimoine immatériel doit être également assurée pendant les déplacements : on sous-estime trop souvent les risques hors du laboratoire. Les points de sensibilisation porteront sur :

Le comportement dans les **transports publics**, et notamment le train ... on conseillera au chercheur d'éviter de faire état de ses travaux de recherche ou d'autres problèmes qui concernent l'institution. Il sera également invité à ne pas laisser son ordinateur dans le compartiment à bagages et s'il travaille dans le train sur son ordinateur, à s'équiper d'un filtre de confidentialité pour éviter que ses voisins ne puissent lire ses informations de connexion, ses e-mails. Enfin, dans la mesure du possible on lui conseillera d'éviter les spots wi-fi publics, particulièrement dans le TGV...

Les missions. Votre chercheur part à **l'étranger** ? Suggérez lui de n'emporter que le minimum de documents nécessaires et si possible, équipez votre laboratoire d'un ordinateur au disque dur vide qui servira à tous les collaborateurs en mission à l'étranger et sera nettoyé à leur retour (il arrive souvent que lors du contrôle douanier à l'aéroport, les ordinateurs soient scannés et les données copiées). A l'hôtel, invitez-le à ne pas laisser son ordinateur dans sa chambre et à ne pas utiliser le réseau wi-fi de l'hôtel. Conseillez-lui la prudence dans ses rencontres et dans les propos qu'il tiendra, surtout dans les pays sensibles.

Vos collaborateurs font une **communication** lors d'un congrès ? Attention au contenu de leurs slides, de leurs posters. Si à l'issue de la présentation, un participant leur demande d'envoyer leurs slides, invitez-les à toujours réclamer les coordonnées complètes de la personne et à vérifier son profil avant l'envoi. Qu'ils soient également discrets dans les propos qu'ils tiennent entre collègues ou lors de rencontres.

Votre laboratoire participe à un **salon** ? Evitez d'apporter des fiches techniques trop détaillées, des documents comportant des informations stratégiques à usage interne. Demandez les coordonnées complètes des personnes à qui vous les remettez. Cela pourra toujours vous être utile

<sup>35</sup> Ernst & Young, Cybersécurité : créer les conditions de la confiance dans le monde digital, 2015.

également par la suite pour faire une relance. Gardez un œil attentif sur vos outils de travail (ordinateur, smartphone, prototype,...).

## 5. Conclusion

---

En conclusion, si le mouvement Open est synonyme de partage, collaboration, co-création ... il n'est pas antinomique avec la protection du patrimoine immatériel. Protéger ses actifs immatériels même dans un environnement « open » innovation, science, data ... c'est combiner des mesures immatérielles telles que les protections juridiques classiques axées sur la propriété intellectuelle et la propriété industrielle, des mesures matérielles telles que la protection des locaux, la sécurité informatique et bien sûr des mesures organisationnelles et humaines.

En fait il s'agit de trouver l'équilibre entre d'une part, une protection des actifs immatériels qui ne soit pas un frein à l'innovation et permette l'agilité, la co-construction et d'autre part, une innovation et une science ouverte qui permettent des retombées économiques dans le pays à la source de l'avancée de la recherche et de l'innovation. Cela suppose que les conditions « structurelles » soient mises en place pour favoriser le transfert technologique, de la recherche à l'innovation technologique, que les freins à la création d'entreprises innovantes soient levés (cadre juridique, financement, etc.), que la mise sur le marché soit facilitée. Sans cela les avancées de la recherche profiteront aux pays émergents dont les équipes de recherche, tout aussi performantes que celles des pays occidentaux et aux salaires moins élevés attireront les investisseurs. Et le rêve décrit par la Commission européenne et repris en préambule de cet article tournera au cauchemar.

## A propos de l'auteur

---



D. Dieng est consultante en Intelligence stratégique (AKASIAS). Sa carrière professionnelle - près de 25 années d'expérience - est constituée d'allers-retours entre l'industrie et les milieux académiques, dans lesquels elle exerce encore aujourd'hui. Son challenge consiste à créer des ponts entre ces deux univers et, dans un environnement de plus en plus compétitif pour la recherche, à transférer aux universités et aux centres de recherche, une démarche qui a fait ses preuves dans l'industrie, à savoir l'intelligence stratégique.



Elle est l'auteur de l'ouvrage "Intelligence Stratégique : guide pour la recherche et l'innovation" (PUN, 2014) et est l'organisatrice de la première conférence belge sur l'intelligence stratégique pour la recherche et l'innovation : <http://is4research.be/>.

Elle intervient également comme formatrice auprès des chercheurs qu'elle sensibilise à l'intelligence stratégique et forme à la veille. Sa formation et son expérience lui permettent une approche holistique sur les 3 piliers de l'intelligence stratégique : veille, protection et influence.

**Contact :** Dominique Dieng - AKASIAS - [dominique.dieng@akasias.eu](mailto:dominique.dieng@akasias.eu) - Tél. +32(0)2 280 14 18 - [www.akasias.eu](http://www.akasias.eu)